IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Jing Xiang et al.
Serial No. 10/791,414
Filed: 03/03/2004
Attorney Docket No. 7000-741
Examiner: Amare F. Tabor
Art Unit: 2434
For: **TECHNIQUE FOR MAINTAINING SECURE NETWORK CONNECTIONS**

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

An **APPEAL BRIEF** is filed herewith. Appellants enclose a payment in the amount of $620.00 as required by 37 C.F.R. § 41.20(b)(2). Appellants also enclose an additional payment in the amount of $150.00 to cover the fee associated with a One-month Extension of Time and request that this be considered a petition therefor. If any additional fees are required in association with this appeal brief, the Director is hereby authorized to charge them to Deposit Account 50-1732, and consider this a petition therefor.

APPEAL BRIEF

(1) REAL PARTY IN INTEREST

The real party in interest is the assignee of record, i.e., Rockstar Bidco, LP, of 1285 Avenue of the Americas, New York, New York 10119-6064, a Delaware Limited Partnership.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of Appellants' knowledge.

(3) STATUS OF CLAIMS

Claims 10-12, 14, 17, 20-25 and 27-28 were rejected with the rejection made final on April 4, 2011.

Claims 11 and 26 were cancelled in the Response to the Final Office Action filed June 6, 2011 ("Response Filed June 6, 2011").

Claims 10, 12, 14, 17, 20-25 and 27-28 are pending and are the subject of this appeal.

(4) STATUS OF AMENDMENTS

The amendments submitted in the Response Filed June 6, 2011 have been entered.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

In the following summary, Appellants have noted where in the Specification certain subject matter exists. Appellants wish to point out that these citations are for demonstrative purposes only and that the Specification may include additional discussion of the various elements, citations to which are not pointed out below. Thus, the noted citations are in no way intended to limit the scope of the pending claims.

Independent claim 10 recites a method for maintaining secure network connections **(see Specification, page 9, lines 5-8)**, the method comprising:

duplicating, at a third network element, a security association associated with a secure network connection between a first network element and a second network element **(see Specification, page 14, lines 11-21; see also Figure 5, elements 500, 502, 504)**, wherein a lookup of the security association associated with the secure network connection is not dependent on any destination address **(see Specification, page 15, lines 6-10)**; and

in response to detecting failure of the second network element, replacing the second network element with the third network element in the secure network connection with the first network element, wherein the secure network connection between the first network element and the third network element is based on the duplicated security association **(see Specification, page 14, line 21 through page 15, line 10)**; and

sending at least one secure message from the third network element to the first network element to notify the first network element that the secure network connection will be taken over by the third network element **(see Specification, page 14, line 22 through page 15, line 2)**.

Independent claim 12 recites a method for maintaining secure network connections, the method comprising **(see Specification, page 9, lines 5-8)**:

configuring a plurality of security gateways such that a lookup of security associations is not dependent on any destination address **(see Specification, page 15, lines 6-10)**;

sharing a security association among the plurality of security gateways **(see Specification, page 14, lines 11-21; see also Figure 5, elements 500, 502, 504)**;

a first of the security gateways detecting failure of a second of the security gateways involved in a secure connection with a network device, wherein the secure network connection is associated with the security association **(see Specification, page 14, line 21 through page 15, line 10)**; and

in response to detecting the failure, the first security gateway sending a message to the network device that the first security gateway is taking over the secure network connection **(see Specification, page 14, line 22 through page 15, line 2)**.

Independent claim 22 recites a first security server comprising **(see Specification, page 14, lines 13-15; see also Figure 5, element 504)**:

a transceiver to receive information relating to at least one security association of a secure network connection between a mobile client and a second security server **(see Figure 4, element 406; see also Specification, page 14, lines 11-21 and Figure 5, elements 500, 502, 504)**; and

a processor module to:

monitor operation of the second security server **(see Specification, page 14, lines 21-22)**;

in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection **(see Specification, page 14, line 22 through page 15, line 2)**; and

communicate with the mobile client using the at least one security association over the secure network connection between the first security server and the mobile client **(see Specification, page 15, lines 6-9)**.

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 10, 12, 14, 17, 20-25 and 27-28 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,966,003 B1 to Joseph et al. (hereinafter "Joseph") in view of U.S. Patent No. 7,020,464 B2 to Bahl et al. (hereinafter "Bahl").

(7) ARGUMENT

A. Introduction

Appellants submit that the Patent Office has not shown where all the elements of the pending claims are shown in the prior art. In particular, the Patent Office has not shown where the prior art discloses or suggests the use of a same secure network connection for subsequent communications by a first network element upon detection of a failure of a second network element with whom the first network element was communicating, or the notification by a third network element to the first network element that the same secure network connection will be taken over by the third network element. As such, Appellants request that the Board reverse the Examiner and further instruct the Examiner to allow the claims for these reasons along with the reasons noted below.

B. Legal Standards

Section 103(a) of the Patent Act provides the statutory basis for an obviousness rejection and reads as follows:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Courts have interpreted 35 U.S.C. § 103(a) as a question of law based on underlying facts. As the Federal Circuit stated:

> Obviousness is ultimately a determination of law based on underlying determinations of fact. These underlying factual determinations include: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) the extent of any proffered objective indicia of nonobviousness.

Monarch Knitting Mach. Corp. v. Sulzer Morat GmBH, 45 U.S.P.Q.2d (BNA) 1977, 1981 (Fed. Cir. 1998) (internal citations omitted).

Once the scope of the prior art is ascertained, the content of the prior art must be properly combined. Initially, the Patent Office must show that there is a suggestion to combine the references. *In re Dembiczak*, 175 F.3d 994 (Fed. Cir. 1999). Even if the Patent Office is able to articulate and support a suggestion to combine the references, it is impermissible to pick and choose elements from the prior art while using the application as a template. *In re Fine*, 837 F.3d 1071 (Fed. Cir. 1988). To reconstruct the invention by such selective extraction constitutes impermissible hindsight. *In re Gorman*, 933 F.2d 982 (Fed. Cir. 1991). After the combination has been made, for a *prima facie* case of obviousness, the combination must still teach or fairly suggest all of the claim elements. *In re Royka*, 490 F.2d 981 (C.C.P.A. 1974); MPEP § 2143.03.

Some elements may be inherent within the reference. "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (quoting *Cont'l Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991)). "The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Id.* (citation and quotation omitted). Thus, the possibility that an element may be derived from the reference is insufficient to establish that the element is inherent to the reference.

Whether an element is implicitly or explicitly taught by a reference or combination of references is open to interpretation. While the Patent Office is entitled to give claim terms their broadest reasonable interpretation, this interpretation is limited by a number of factors. First, the interpretation must be consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000); MPEP § 2111. Second, the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *In re Cortright*, 165 F.3d 1353, 1359, (Fed. Cir. 1999); MPEP § 2111. Finally, the interpretation must be reasonable. *In re American Academy of Science Tech Center*, 367 F.3d 1359, 1369 (Fed. Cir. 2004); MPEP § 2111.01. This means that the words of the claim must be given their plain meaning unless Appellant has provided a clear definition in the specification. *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989).

If a claim element is missing after the combination is made, then the combination does not render obvious the claimed invention, and the claims are allowable. As stated by the Federal Circuit, "[if] the PTO fails to meet this burden, then the applicant is entitled to the patent." *In re Glaug,* 283 F.3d 1335, 1338 (Fed. Cir. 2002).

C. Claims 10, 12, 14, 17, 20-25 and 27-28 Are Patentable Over Joseph and Bahl

Claims 10, 12, 14, 17, 20-25 and 27-28 were rejected under 35 U.S.C. § 103(a). Appellants respectfully traverse. The standards for obviousness are set forth above.

Claim 10

Appellants' claim 10 relates to an embodiment wherein a secure connection between a first network element and a second network element is established, and in response to detecting failure of the second network element, the second network element is replaced with the third network element. The same secure network connection, which was used between the first network element and the second network element prior to the failure, is used between the first network element and the third network element subsequent to the failure. Thus, no new secure network connection between the first network element and the third network element is established.

Moreover, the third network element sends a secure message to the first network element notifying the first network element that the secure connection will be taken over by the third network element. Among other features, this allows the first network element to address subsequent messages to the third network element rather than to the second network element.

Neither Joseph nor Bahl, alone or in combination, teach or suggest this combination of features. The Patent Office asserts that Joseph discloses the feature of detecting failure of a second network element and in response, replacing the second network element with a third network element, while using the same secure connection (Final Office Action mailed April 4, 2010 (hereinafter "Final Office Action"), pp. 2–3). Appellants respectfully disagree with this interpretation for at least the following reasons. First, regarding terminology, Appellants note that Joseph never uses the term "connection." Joseph does however use terms such as "secure communication," "first secure communication," and "second secure communication" (Joseph,

col. 2, ll. 23 – 42). Appellants believe that the Patent Office interprets such "communication" to be analogous to Appellants' recited "secure connection."

Joseph, at column 4, line 58 – column 5, line 17, discloses that it may be determined that a "first communication" between a first network device and third network device has failed. In response, a "second communication" between the first network device and the third network device is established. Thus, Joseph explicitly states that the first communication is not used between the first network device and the second network device. If, as the Patent Office appears to assert, the "communications" discussed in Joseph are analogous to Appellants' recited "secure connection," it is quite clear that Joseph does not disclose using the same secure connection between the first device and the third device, because Joseph explicitly discloses that a "second communication … between the first and third network devices … is established" (Joseph, col. 4, ll. 63–65). Joseph emphasizes this by disclosing that "the transition from the first communication to the second communication will occur transparently…" (Joseph, col. 5, ll. 12–13; emphasis added). Appellants submit that a "transition" (transparent or not) is not necessary if the same secure connection is utilized. In contrast, Appellants' claim 10 explicitly recites that the second network element is replaced with the third network element "*in the secure network connection with the first network element*" (emphasis added).

In the Advisory Action mailed June 27, 2011 (hereinafter "Advisory Action"), the Patent Office asserts "Examiner … notes that claim 10 does not recite 'the same secure connection' either" (Continuation Sheet, ll. 2-3). In response, Appellants note that only one secure network connection is recited in claim 10, and the article "the" is used to indicate the previously recited secure network connection is used between the first network element and the third network element. Appellants submit that no reasonable interpretation of this claim language could conclude that the subsequently recited secure network connection is not the same as the initially recited secure network connection.

Because Appellants' claim 10 recites the use of the same secure network connection between two different sets of network elements, and Joseph explicitly discloses that different first and second "communications" are used in such a situation, Appellants submit that claim 10 is not rendered obvious by the cited references.

In addition to the distinction discussed above, Appellants' claim 10 further recites that upon replacing the second network element with the third network element, at least one secure

message is sent from the third network element to the first network element to notify the first network element that the secure network connection will be taken over by the third network element. Neither Joseph nor Bahl teaches this feature. When addressing this limitation in the Final Office Action, the Patent Office asserted that this feature is disclosed by the "second communication" discussed above (Final Office Action, pp. 3–4). But it is clear that the term "communication" is used in Joseph to mean something similar to a conversation and does not relate to any particular message. For example, Joseph discloses "[a]s the second communication proceeds, the sequence number for each message packet are checked…" (Joseph, col. 5, ll. 27-28). Therefore, the disclosure of a "second communication" does not refer to any particular message as suggested by the Patent Office, nor does Joseph otherwise suggest that the third network device "[sends] *at least one secure message from the third network element to the first network element to notify the first network element that the secure network connection will be taken over by the third network element*" (emphasis added), as recited in Appellants' claim 10. In particular, Joseph does not teach or suggest in any capacity that the third device notifies the first device when taking over a connection/communication.

In the Advisory Action, the Patent Office suggests that this feature is inherent "because the first element would not recognize the third network element communication request [e.g. 34 (FIG. 1)] unless it is notified first." In response, Appellants submit that a feature is inherent only if that is the only means by which it could be accomplished. In Joseph, not only is this feature not inherent, but Joseph explicitly provides an alternative mechanism for communications subsequent to a failure. In fact, a close examination of Joseph suggests that not only is the first network device not notified that the third network device is taking over for the second network device, but that it is not even aware of the third network device. In particular, Joseph discloses that a switch 54 initially routes traffic between the first network device (a device, such as a phone, on an egress network 42) and a second network device (a blade 52). Upon failure of the blade 52, traffic from the egress network 42 (i.e., traffic from the phone) is "redirected" to the standby blade 52′ (Joseph, col. 7, ll. 27–47). Appellants submit that if traffic is "redirected," then clearly the phone on the egress network 42 is not even aware of the standby blade 52′—otherwise, the phone on the egress network 42 would direct subsequent traffic to the standby blade 52′ directly, and traffic would not need to be redirected. Clearly, the standby blade 52′ is not "*sending at least one secure message…to the first network element to notify the first network*

element that the secure network connection will be taken over." For at least the foregoing reasons, Appellants submit that claim 10 is allowable over the cited references.

Claims 12 and 22

Appellants' claim 12 recites certain features that are analogous to those discussed herein with regard to claim 10, and Appellants' arguments above are equally applicable with regard to claim 12. In particular, claim 12 recites that a first security gateway is "*taking over the secure network connection*" between a second security gateway and a network device. As discussed above, Joseph discloses the use of two separate and distinct communications; Joseph does not disclose an ability to utilize the same secure connection. Claim 12 also recites that the first security gateway sends "*a message to the network device that the first security gateway is taking over the secure network connection.*" As discussed above, Joseph fails to teach or suggest that the standby blade 52′ sends a message to the egress network that the standby blade 52′ is "*taking over the secure network connection.*" Instead, Joseph discloses a different process wherein traffic directed toward the failed blade is redirected by a switch to the standby blade 52′. For at least the foregoing reasons, Appellants submit that claim 12 is allowable over the cited references. Claim 22 is a server embodiment of claim 12 and contains limitations analogous to those discussed herein with regard to claim 12. Therefore, claim 22 should be allowable for the same reasons discussed with regard to claim 12.

Claims 20, 21, 23, 26, and 27 depend directly or indirectly from claim 10, and thus include all of the features and limitations of claim 10, and are therefore allowable for at least the reason that such claims depend from an allowable independent claim. Claim 25 depends directly or indirectly from claim 12, and thus includes all of the features and limitations of claim 12, and should therefore be allowable for at least the reason that such claim depends from an allowable independent claim. Claims 14, 17, 24, and 28 depend directly or indirectly from claim 22, and thus include all of the features and limitations of claim 10, and should therefore be allowable for at least the reason that such claims depend from an allowable independent claim.

E. Conclusion

As set forth above, none of the cited references, either alone or in combination, disclose or suggest the use of a same secure network connection for subsequent communications by a first

network element upon detection of a failure of a second network element with whom the first network element was communicating, or the notification by a third network element to the first network element that the same secure network connection will be taken over by the third network element. As such, Appellants request that the Board reverse the Examiner and instruct the Examiner to allow the claims.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By: /Eric P. Jensen/

Eric P. Jensen
Registration No. 37,647
100 Regency Forest Drive, Suite 160
Cary, NC 27518
Telephone: (919) 238-2300

Date: November 3, 2011
Attorney Docket: 7000-741

(8) CLAIMS APPENDIX

1. – 9. (Cancelled)

10. A method for maintaining secure network connections, the method comprising:

duplicating, at a third network element, a security association associated with a secure network connection between a first network element and a second network element, wherein a lookup of the security association associated with the secure network connection is not dependent on any destination address; and

in response to detecting failure of the second network element, replacing the second network element with the third network element in the secure network connection with the first network element, wherein the secure network connection between the first network element and the third network element is based on the duplicated security association; and

sending at least one secure message from the third network element to the first network element to notify the first network element that the secure network connection will be taken over by the third network element.

11. (Cancelled)

12. A method for maintaining secure network connections, the method comprising:

configuring a plurality of security gateways such that a lookup of security associations is not dependent on any destination address;

sharing a security association among the plurality of security gateways;

a first of the security gateways detecting failure of a second of the security gateways involved in a secure connection with a network device, wherein the secure network connection is associated with the security association; and

in response to detecting the failure, the first security gateway sending a message to the network device that the first security gateway is taking over the secure network connection.

13. (Cancelled)

14. The first security server according to claim 22, wherein a lookup of security associations is not dependent on any destination address.

15. – 16. (Cancelled)

17. The first security server according to claim 22, wherein communications between the mobile client and the first security server are based on a security architecture for the internet protocol (IPsec).

18. – 19. (Cancelled)

20. The method of claim 10, further comprising:

during life of the secure network connection between the first and second network elements, the third network element receiving information relating to the security association of the secure network connection from the second network element.

21. The method of claim 20, wherein the first network element is a mobile client, and the second and third network elements are security servers.

22. A first security server comprising:

a transceiver to receive information relating to at least one security association of a secure network connection between a mobile client and a second security server; and

a processor module to:

monitor operation of the second security server;

in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection; and

communicate with the mobile client using the at least one security association over the secure network connection between the first security server and the mobile client.

23. The method of claim 10, wherein the first network element is a mobile client, and the second and third network elements are security servers.

24. The first security server of claim 22, wherein information relating to the at least one security association is duplicated at the first and second security servers.

25. The method of claim 12, wherein sharing the security association comprises sharing an IPsec security association among the plurality of security gateways.

26. (Cancelled)

27. The method of claim 10, further comprising:

after replacing the second network element within the third network element in the secure network connection, the third network element communicating with the first network element without the third network element re-establishing another connection with the first network element.

28. The first security server of claim 22, wherein the processor module is configured to communicate with the mobile client after taking over the secure network connection without re-establishing a new connection.

(9) EVIDENCE APPENDIX

Appellants rely on no evidence, thus this appendix is not applicable.

(10) RELATED PROCEEDINGS APPENDIX

As there are no related proceedings, this appendix is not applicable.